DMS/MGS End Users Quick Reference Guide for MS Outlook Express

Overview: User Responsibilities

MGS End User Role

A PKI end user is an individual that registers with the PKI Certificate Authority (CA) to acquire public/private keys. These keys are used to sign and encrypt documents transmitted between computer systems.

MGS End User Responsibilities

Protects his or her private key from disclosure.
Interacts with the Local Registration Authority (LRA) to obtain his/her Registration Form/Instructions.
Reports any loss or compromise of his/her private key.
Complies with established policy regarding use of his/her private key.

Desktop Preparation:

Workstation requirements

OS: Win 95, 98, 98 v 2 or Windows NT v 4 with (SP4 128 bit Encryption)
Email Client: Outlook Express 5
Browser: Internet Explorer (IE) v 5 or higher
3 1/2" Floppy Disk Drive

Before Proceeding: (Additional Info See pages MGS Users Guide pages 2 - 67)

Download & store your Identity and Email Certificates (*.p12) on a Floppy Disk.
Also store a copy of the DOD PKI Root Certificate (dodroot.p7b) on the Floppy Disk.
Disk will contain 3 files. Keep for backup.

Enable Outlook Express is a 4 Step Process: (pages 67 - 142)

Step 1: Install the DOD PKI Root Certificate in the Operating System
Step 2: Install your Email Certificate in the Operating System
Step 3: Configure an Outlook Security Profile in Outlook Express 5.
Step 4: Install your Identity Certificate in the Operating System

Install DOD PKI Root Certificate (pages 68 - 76)

Step 1. Insert the floppy disk with the exported certificates into your workstation's floppy drive.
Step 2. Double click on the "dodroot.p7b" file
Step 3. The Certificate Manager Import Wizard will appear. Click the *Next* button to start importing the certificate.
Step 4. Select the *Automatically select the certificate store based on the type of certificate* option.
Step 5. Click the *Next* button to continue.
Step 6. Click the *Finish* button to continue.
Step 7. Press the *Yes* button to confirm the installation of the certificate.
Step 8. Certificate installed, press the *OK* button to continue.

Install DOD PKI Email Certificate (pages 77 - 101)

Step 1. Using the floppy disk with the exported certificates. Select the *floppy drive (A:)* in Windows Explorer.
Step 2. Double click on the file containing your DoD E-mail Certificate
Step 3. The Certificate Manager Import Wizard will appear. Click the *Next* button to start importing the certificate.
Step 4. Click the *Next* button to continue.
Step 5. Enter the password you used to protect your E-Mail Certificate when you exported it from Netscape.
Step 6. Check both the *Enable strong private key protection* and *Mark the private key as exportable* boxes.
Step 7. Click the *Next* button to continue.
Step 8. Select the *Place all certificates into the following store* option.
Step 9. Click the *Browse* button.
Step 10. Click the *Personal* folder in the Select Certificate Store window.
Step 11. Click *OK* to continue.
Step 12. Click the *Next* button to continue.
Step 13. Click the *Finish* button to continue.
Step 14. The Private Key Container window will appear. Click the *Set Security Level...* button.
Step 15. Select the *High* option.
Step 16. Click the *Next* button to continue.
Step 17. Select *Create a new password for this item*.
Step 18. Enter your Last Name in the *Password for:* field.
Step 19. Select a password to protect your Certificates. Enter this password in the *Password:* field.
Step 20. Confirm the password & click the *Finish* button to continue.
Step 21. The Private Key Container window will appear. Enter the password you created.
Step 22. Ensure that the *Remember password* option is **NOT** checked.
Step 23. Click *OK* to continue.
Step 24. Import Successful, Click *OK* to continue.

Configure Outlook Express 5 Security Profile (Pages 102 - 117)

Step 1. Open MS Outlook Express
Step 2. In the *Tools* pull-down menu, select the *Accounts* menu item.
Step 3. The Internet Accounts window will appear. Click on the *Mail* tab.
Step 4. The user's mail account should be present. Highlight your mail account and click on *Properties*. (To setup a new account contact your System Administrator.)
Step 5. The Properties window for your mail account will appear. Click the *Security* tab.
Step 6. Check *Use a digital ID when sending secure messages from:* (your email account should be present under the checkbox). Click on the *Digital ID…* button
Step 7. Click on the row containing the certificate issued by either *Med Email CA-1* or *Med Email CA-2* to highlight the certificate. Click the *OK* button.
Step 8. The user is returned to the account Properties window. The certificate should appear in the box next to the *Digital ID…* button. Click *OK.*
Step 9. User is returned to the Internet Accounts window, click *Close* to return to Outlook Express.
Step 10. In the *Tools* menu, choose the *Options* menu item.
Step 11. The Options window appears. Select the *Security* tab.
Step 12. Click the *Advanced…* button.
Step 13. Set the Encryption level to *3DES*.
Step 14. Check *Include my digital ID when sending signed messages* and *Add senders' certificates to my address book*. Click *OK.*
Step 15. User is returned to the Options window Security tab. Check the *Digitally sign all outgoing messages* box, then click *OK.*
Step 16. The user is returned to Outlook Express. Close Outlook Express and return to Windows Explorer to install the ID Certificate.

Install ID Certificate: (Not required for MGS) (MGS Users Guide Pages 118 - 142)

Step 1. From the floppy, double click on the file containing your DOD ID Certificate. The Certificate Manager Import Wizard will appear. Click the *Next* button to continue.
Step 2. Click the *Next* button to continue.
Step 3. Enter the password you used to protect your ID Certificate when you exported it from Netscape.
Step 4. Check both the *Enable strong private key protection* and *Mark the private key as exportable* boxes.
Step 5. Click the *Next* button to continue.
Step 6. Select the *Place all certificates into the following store* option.
Step 7. Click the *Browse* button.
Step 8. Click the *Personal* folder in the Select Certificate Store window.
Step 9. Click *OK* to continue.
Step 10. Click the *Next* button to continue.
Step 11. Click the *Finish* button to continue.
Step 12. The Private Key Container window will appear. Click the *Set Security Level…* button.
Step 13. Select the *High* option.
Step 14. Click the *Next* button to continue.
Step 15. **Select *Use this password to access this item.* Click Finished.
Step 16. Enter the password your created to use your email certificate in the *Password for…* field.
Step 17. Ensure that the *Remember password* option is **NOT** checked and click *OK* to continue.
Step 18. Import Successful. Click *OK* to continue.

**Refer to MGS Users Guide Page 134 to choose different passwords for each certificate.

Sending Signed Mail Using DMS/MGS: (pages 143 - 146)

Step 1. Open MS Outlook Express 5. Highlight the *Inbox* and click *New Mail.*
Step 2. Address and type message. When finished click *Send.*
Step 3. Enter the password created when installing the email certificate. Click *OK* and the message will be sent. **Do Not** check *Remember Password.*
Step 4. The user will be returned to the Inbox.

Receiving Signed Mail Using DMS/MGS: (pages 147 - 156)

Step 1. In the Inbox, a signed message has a red ribbon on the *Envelope* icon. The preview pane also shows the message is signed. Double click on the message to open.
Step 2. Again the message is identify as signed. Click on *Continue* to read the message.
Step 3. The message is now readable. Under the subject line, a security line shows the status of the message.
Step 4. Right mouse click on the red ribbon icon and select *View the Signing Digital ID.*
Step 5. Certificate information can be viewed, click *OK* when finished. The user will be returned to the signed message.
Step 6. Sent messages can provide recipients access to sender's public keys. When a message is received an address book entry is created. Click on the *Address Book* button.
Step 7. The Address Book is displayed. Highlight an address book entry and double click for additional information.
Step 8. The Properties of the address book entry are displayed. Click on the *Digital ID's* tab.
Step 9. Verify the public key was delivered. The user may now send encrypted mail to this addressee. Click *OK* to close the properties window. Exit from the address book to return to the signed message.
Step 10. If the window is empty after receiving a signed message or a signed message has not been received from a person to whom the user wishes to send encrypted mail, the user must go to the DOD PKI web site to retrieve a public key.

Retrieving Other Users Certificates from DOD PKI Website: (pages 158 - 176)

Step 1. Open Microsoft Internet Explorer Version 4.01 or greater.
Step 2. Type http://ds-2-ent.den.disa.mil/ in the *Address* field and press *Enter*.
Step 3. Once the page has loaded, click on *Search the Mail Directory Server*.
Step 4. Ensure *People* is selected in the *Find* drop down menu.
Step 5. Type in the last name of the person you wish to receive the certificate for in the *Search For:* field.
Step 6. Click the *Search* button.
Step 7. Once the screen has loaded with the results of the search, review the information to ensure the certificate is for the correct person.
Step 8. Click on *Download Certificate*.
Step 9. A *File Download* window will appear. Select the *Save this file to disk* option.
Step 10. Click the *OK* button to continue.
Step 11. A *Save As* window appear. In the *File name* field enter the person's last name followed by their first initial and a .cer extension (for example smitht.cer for Tom Smith).
Step 12. Click the *Save* button to save the Certificate to your workstation.
Step 13. If not already running, launch MS Outlook Express 5. Open the Address Book and click on *New* button, then click the *New Contact* menu item.
Step 14. Add contact information into address book, then click on the *Digital IDs* tab.
Step 15. Click on *Import* button, a window will open requesting the user to select a file to open.
Step 16. Select the file downloaded (*.cer) from the DOD PKI website. Click *Open*.
Step 17. The certificate will be loaded into the window below with a green checkmark. Click *OK*, then close the address book. The user is able to send encrypted mail to the addressee.

Sending Encrypted Mail with DMS/MGS: (pages 177 - 179)

Step 1. Open Outlook Express and start a new message by clicking on the *New Mail* button on the toolbar.
Step 2. Address to a recipient in your address book and type a message, when finished make sure both the *Sign* and *Encrypt* buttons on the toolbar are pressed then click *Send*.
Step 3. User must now enter their private key password to sign the message and then click *OK*. The message is then sent and the user is returned to the inbox.

Receiving Encrypted Mail with DMS/MGS: (pages 180 - 183)

Step 1. In the user's inbox an encrypted message is identified by a blue lock on the message envelope icon. Highlight the message and a password prompt will appear.
Step 2. Enter the password and click *OK*. The message information will appear in the preview pane. Double click the message to open; another password screen may appear. Re-enter the password.
Step 3. When message is open the user will again see the security information displayed. Click the *Continue* button to read the message.

HELP (page 184)

24hr x 7days:	PKI Help Desk Support. DSN is 570-5690.
0800 – 1700 Eastern Time:	MGS Lab (703) 824-4620
MGS Web Site:	http://falcon3.ncr.disa.mil
PKI Web Site:	http://ds-2-ent.den.disa.mil